

CLAIMS

What is claimed is:

1 1. *In a video device, a method comprising:*
2 *continuously clocking a cipher unit, upon power on/reset, to introduce entropy*
3 *into the cipher unit;*
4 *in response to a subsequent request after n clocks for a first pseudo random*
5 *number, where n is an integer, taking a first plurality of output bits of the cipher unit*
6 *and storing the first output bits;*
7 *upon storing the first output bits, outputting the stored first output bits as the*
8 *first pseudo random number; and*
9 *transitioning to a selected one of the continuously clocking state, another*
10 *output taking state, and an authenticated state depending on whether upon*
11 *provision of the first pseudo random number, an indication of an unsuccessful*
12 *authentication using the first pseudo random number, another request for a second*
13 *pseudo random number, or an indication of a successful authentication using the*
14 *first pseudo random number is received.*

1 2. *The method of claim 1, wherein the method further comprises*
2 *taking a second plurality of output bits of the cipher unit, while in said another*
3 *output taking state, and storing the second output bits; and*
4 *upon storing the second output bits, outputting the stored second output bits*
5 *as the second pseudo random number.*

1 3. *The method of claim 1, wherein the method further comprises*

2 *receiving another request for a third pseudo random number, while in said*
3 *authenticated state;*
4 *transition to said another output taking state.*

1 4. *The method of claim 1, wherein the method further comprises*
2 *receiving a selected one of an unauthenticated notification and a detachment*
3 *notification, while in said authenticated state; and*
4 *transition to said continuously clocking state.*

1 5. *A video apparatus comprising:*
2 *a cipher unit to generate a sequence of ciphering bits to cipher video to be*
3 *transmitted by the video apparatus; and*
4 *a state machine coupled to the cipher unit to also use the ciphering unit to*
5 *generate pseudo random numbers to authenticate video receiving devices attached*
6 *to said video apparatus.*

1 6. *The video apparatus of claim 5, wherein the state machine is equipped to*
2 *transition to a continuous clocking state, upon power on/reset, and causes the*
3 *cipher unit to be continuously clocked to introduce entropy into the cipher unit.*

1 7. *The video apparatus of claim 6, wherein the state machine is further*
2 *equipped to transition from said continuous clocking state to a first output taking*
3 *state, in response to a subsequent request after n clocks for a first pseudo random*
4 *number, where n is an integer, to take a first plurality of output bits of the cipher unit,*
5 *and store the taken first output bits.*

1 8. *The video apparatus of claim 7, wherein the state machine is further
2 equipped to transition from said first output taking state to an output state, upon
3 storing the first output bits, to output the stored first output bits as the first pseudo
4 random number.*

1 9. *The video apparatus of claim 8, wherein the state machine is further
2 equipped to transition from said output state to a selected one of the continuously
3 clocking state, a second output taking state, and an authenticated state depending
4 on whether upon provision of the first pseudo random number, an indication of an
5 unsuccessful authentication using the first pseudo random number, another request
6 for a second pseudo random number, or an indication of a successful authentication
7 using the first pseudo random number is received.*

1 10. *The video apparatus of claim 9, wherein the state machine is further
2 equipped to transition from said second output taking state to said output state upon
3 taking a second plurality of output bits of the cipher unit and storing the second
4 output bits.*

1 11. *The video apparatus of claim 9, wherein the state machine is further
2 equipped to transition from said authenticated state to said another output taking
3 state upon receiving another request for a third pseudo random number.*

1 12. *The video apparatus of claim 9, wherein the state machine is further
2 equipped to transition from said authenticated state to said continuously clocking
3 state upon receiving a selected one of an unauthenticated notification and a
4 detachment notification.*

1 13. *A pseudo random number generator comprising:*
2 *a cipher unit to generate a sequence of ciphering bits to cipher a stream of*
3 *data; and*
4 *a state machine coupled to the cipher unit to also use the ciphering unit*
5 *generate a plurality of pseudo random numbers based on selected ones of said*
6 *cipher bits.*

1 14. *The pseudo random generator of claim 13, wherein the state machine*
2 *operates in a selected one of a continuous clocking state, a first cipher bit taking*
3 *state, an output state, a second cipher bit taking state, and an authenticated state,*
4 *wherein the state machine causes the cipher unit to be continuously clocked while in*
5 *said continuous clocking state to introduce entropy in said cipher unit, causes first*
6 *and second plurality of said cipher bits to be taken and stored, in said first and*
7 *second cipher bit taking states respectively, causes the stored first/second cipher*
8 *bits to be output as first/second random numbers, causes the cipher bits of the*
9 *cipher unit to be used to cipher said stream of data during said authenticated state.*

1 15. *The pseudo random generator of claim 14, wherein the state machine is*
2 *equipped to transition from said continuous clocking state to said first output taking*
3 *state, in response to a subsequent request after n clocks for said first pseudo*
4 *random number, where n is an integer, and to transition from said first output taking*
5 *state to said output state, upon storing the first output cipher bits.*

1 16. *The pseudo random generator of claim 14, wherein the state machine is*
2 *equipped to transition from said output state to a selected one of the continuously*

3 *clocking state, the second output taking state, and the authenticated state*
4 *depending on whether upon provision of the first pseudo random number, an*
5 *indication of an unsuccessful authentication using the first pseudo random number,*
6 *another request for a second pseudo random number, or an indication of a*
7 *successful authentication using the first pseudo random number is received.*

1 17. *The pseudo random generator of claim 14, wherein the state machine is*
2 *equipped to transition from said second output taking state to said output state upon*
3 *taking the second plurality of output cipher bits of the cipher unit and storing the*
4 *second output cipher bits.*

1 18. *The pseudo random number generator of claim 14, wherein the state*
2 *machine is further equipped to transition from said authenticated state to said*
3 *second output taking state upon receiving another request for a third pseudo*
4 *random number, and to said continuously clocking state upon receiving a selected*
5 *one of an unauthenticated notification and a detachment notification.*